Application No.: 10/680,400
Attorney Docket No: 14846-28

Reply Under 37 CFR 1.116
Expedited Procedure
Tech. Center: 2131

Amendments to the Claims:

The following listing of claims replaces all prior versions, and listings, of claims in the present application. Please add claim 13. Please cancel claims 2, 4, 5, 11, and 12. Please amend claims 1 and 10 as follows:

Listing of the Claims:

1. (currently amended) A method for ~~effecting controlled~~ allowing a user to temporarily gain access to a privileged account on a computer system to perform a maintenance task, the method being a replacement for a conventional switch user command, comprising:

receiving a switch user command login ~~into an account~~ with a user id and an account name as an argument;

retrieving a list of privileged account names;

determining whether the account name is in a list of privileged account names and ~~allowing access to the account~~ diverting the user to the conventional switch user command prompt if the account name is not in the privileged account list; otherwise,

determining whether the user id ~~is in a list of user ids~~ belongs to a privileged group located in a group list on the computer system having permission to access privileged accounts;

denying access to privileged accounts and notifying the manager if the user id does not belong to the privileged group, otherwise,

allowing access to the account ~~if the user id is in the list of user ids having permission to access privileged accounts~~;

prompting for a reason for accessing the account;

recording a reason for accessing the account;

notifying a manager by email of the access of the privileged account of the switch user login along with the name of a first log file;

recording keystrokes in [[a]] the first log file while logged into the account;

recording keystrokes in a duplicate log file while logged into the account;

Application No.: 10/680,400
Attorney Docket No: 14846-28

Reply Under 37 CFR 1.116
Expedited Procedure
Tech. Center: 2131

<u>determining whether the first log file was tampered with and, if so, recording that the first</u> <u>log file was tampered with in the duplicate log file and transmitting the duplicate log file to the</u> <u>manager;</u>

terminating the <u>switch user</u> login;

and notifying the manager <u>by email</u> of the privileged account of the <u>switch user</u> login termination.

2. (cancelled)

3. (original) A method in accordance with claim 1 further comprising: denying write permission to the log file after the step of terminating the login.

4. (cancelled)

5. (cancelled)

6. (original) A method in accordance with claim 1 further comprising: transmitting the log file to the account manager.

7. (original) A method in accordance with claim 1 further comprising: receiving a password in order to access the privileged account; determining whether the password associated with the user id matches the entered password; and permitting access only if the password associated with the user id matches the entered password.

8. (original) A method in accordance with claim 1 further comprising: notifying the manager of the privileged account if the login is not successful.

9. (original) A method in accordance with claim 1 further comprising: compressing the log file after terminating the login.

Application No.: 10/680,400
Attorney Docket No: 14846-28

Reply Under 37 CFR 1.116
Expedited Procedure
Tech. Center: 2131

10.   (currently amended)   A method in accordance with claim 1 further comprising: recording keystrokes while accessing the account in a duplicate log file; deleting the duplicate log file responsive to a determination that the log file has not been tampered with.

11.   (cancelled)

12.   (cancelled)

13.   (new)   A method for allowing a user to temporarily gain access to a privileged account on a computer system to perform a maintenance task, the method being a replacement for a conventional switch user command, comprising:

receiving a switch user command login with a user id and an account name as an argument;

retrieving a list of privileged account names;

determining whether the account name is in a list of privileged account names and diverting the user to the conventional switch user command prompt if the account name is not in the privileged account list; otherwise,

determining whether the user id is in a list of user ids having permission to access privileged accounts and allowing access to the account if the user id is in the list of user ids having permission to access privileged accounts;

prompting for a reason for accessing the account;

recording a reason for accessing the account;

notifying a manager of the privileged account of the login;

recording keystrokes in a log file while logged into the account;

terminating the login;

and notifying the manager of the privileged account of the login termination.